UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA, Plaintiff, v. PAIGE THOMPSON, Defendant.	Case No. CR19-159-RSL ORDER DENYING MOTION TO STRIKE AND SEVER

This matter comes before the Court on defendant's "Motion to Strike the Crypto Mining Allegations of Count One and to Sever Count Eight of the Indictment" (Dkt. # 124).[1] Having reviewed the submissions of the parties and the remainder of the record, the Court finds as follows:

I. Threshold Matters

As threshold matters, the Court considers (A) the parties' motions to file overlength, (B) the parties' motions to seal, and (C) defendant's motion to strike.

[1] The government introduced a Second Superseding Indictment (Dkt. # 166) after briefing for this motion was submitted. The Second Superseding Indictment modifies the cryptomining allegations contained in Count 1 and Count 8. However, as the Court finds that these modifications do not render the present motion moot, the Court reads the arguments in the present motion as applying equally to both versions of the Superseding Indictment and applies this ruling to the Second Superseding Indictment.

A. Motions to File Overlength

The Court grants the government's "Motion to File a Brief in Excess of Twelve Pages" (Dkt. # 136). The government may file a sixteen-page response. The Court also grants defendant's "Motion to File Overlength Reply Re Defense Motion to Strike Count 1 and Sever Count 8" (Dkt. # 161). Defendant may file an eight-page reply.

B. Motions to Seal

The Court finds that there are compelling reasons to permit filing Exhibits 1, 2, 3, and 4 (Dkt. # 164) to defendant's reply (Dkt. # 163) under seal. The Court therefore grants defendant's "Motion to Seal Exhibits to Defendant's Reply to Government's Response to Motion to Strike Count 1 and Sever Count 8" (Dkt. # 162).

The Court finds that Exhibit A (Dkt. # 176) to the government's supplemental filing (Dkt. # 175) contains Protected Material as defined in the protective order entered on October 30, 2019 (Dkt. # 66). The Court therefore grants the government's "Motion to Seal Exhibit A to Supplemental Filing Relating to Defendant's Motion to Strike Cryptojacking Allegations and to Sever Count 8" (Dkt. # 174).

C. Motion to Strike Surreply

Four days after the defense filed its reply (Dkt. # 163), the government filed a supplemental filing (Dkt. # 175) disputing the defense's assertion that there is no evidence that defendant used the servers belonging to Victims 7 and 8 to perform cryptojacking. The defense filed a "Motion to Strike Government's Surreply" (Dkt. # 184), arguing that the government's supplemental filing is in fact an unauthorized surreply and should therefore be stricken.

Defendant's argument is entirely grounded in LCR 7(g), which provides that a party may file a surreply for the sole purpose of requesting that the court strike material in or attached to the reply. *See* Local Rules W.D. Wash. LCR 7(g). However, LCR 7(g) is local civil rule and does not govern in criminal proceedings. *See* Local Rules W.D. Wash. CrR 1(a) (listing local civil rules that apply to criminal matters). While the Court agrees that the government's filing is properly viewed as a surreply, the governing procedural rules are silent on the government's ability to file such a surreply. *See* Local Rules W.D. Wash. CrR 12; Fed. R. Crim. P. 12, 47.

Because there is no controlling law, the Court may exercise its discretion to determine whether to strike the government's surreply. *See* Fed. R. Crim. P. 57(b). The Court considers the substantive paragraphs of the surreply in turn.

Paragraph 2 of the government's surreply addresses defendant's argument that there is no evidence that defendant's alleged cryptomining activities caused damage to any of the victims enumerated in the indictment. *See* Dkt. # 175 at 1-2. However, defendant raised this argument in her motion. *See* Dkt. # 124 at 6 ("[T]he defense is aware of no evidence that Ms. Thompson's alleged crypto mining utilizing AWS servers caused any of the victims enumerated in the Indictment any damage, such as an increased invoice for usage."). The government does not explain why it was unable to respond to this argument until its surreply. Paragraph 2 of the government's surreply is therefore properly stricken.

However, paragraph 3 and Exhibit A of the government's surreply go to defendant's argument that there is no evidence in general that she used the enumerated victim's servers for cryptomining. *See* Dkt. # 175 at 2. Defendant did not raise this argument until her reply. *See* Dkt. # 163 at 3, 6-8. Given the Court's preference for deciding disputes on the merits, the Court concludes that consideration of paragraph 3 and Exhibit A of the government's surreply is appropriate.

Defendant's motion to strike (Dkt. # 184) is therefore granted in part and denied in part.

II. Motion to Strike Cryptomining Allegations of Count 1 and Sever Count 8

Defendant seeks to eliminate references to her alleged cryptomining from the indictment. She therefore moves the Court to: (A) strike the cryptomining allegations contained in Count 1, and (B) sever the cryptomining-based Count 8.

A. Count 1

Defendant argues that the Court should strike the cryptomining allegations contained in Count 1 because they are unrelated to the government's primary theory of wire fraud alleged in Count 1 – namely, that defendant stole victim data hosted on Amazon Web Services (AWS) servers – and therefore are included only to prejudicially confuse the jury regarding the elements of wire fraud.

Pursuant to Federal Rule of Criminal Procedure 7(d), “Upon the defendant's motion, the court may strike surplusage from the indictment or information.” Fed. R. Crim. P. 7(d). “The purpose of a motion to strike under Fed. R. Crim. P. 7(d) is to protect a defendant against prejudicial or inflammatory allegations that are neither relevant nor material to the charges.”[2] *United States v. Laurienti*, 611 F.3d 530, 546-47 (9th Cir. 2010) (quoting *United States v. Terrigno*, 838 F.2d 371, 373 (9th Cir. 1988)). Accordingly, the Court should exercise its discretion to strike surplusage under Rule 7(d) if the allegations are (1) immaterial *and* irrelevant, and (2) prejudicial *or* inflammatory.

1. Immaterial and Irrelevant

The defense has failed to show that the cryptomining allegations of Count 1 are immaterial and irrelevant to the government’s wire fraud case. Allegations that are material or relevant are not surplusage and should remain unstruck. *See*, *e.g.*, *Laurienti*, 611 F.3d at 547 (holding that allegation that practices were “unlawful” was not surplusage because it was relevant, even if it may have been prejudicial); *Terrigno*, 838 F.3d at 373-74 (holding that prejudicial allegations that funds were destined for the “poor and homeless,” that defendant issued checks “willfully,” and that defendant acted in an effort to “lull and deceive” were not surplusage because they were relevant and material to the charges of embezzlement and conversion).

Count 1 charges defendant with wire fraud in violation of 18 U.S.C. § 1343. The elements of wire fraud are: (1) a scheme to defraud; (2) the use of a wire, radio, or television to further the scheme; and (3) a specific intent to defraud. *United States v. Lindsey*, 850 F.3d 1009, 1013 (9th Cir. 2017).[3] The scheme to defraud must be a deceptive scheme to deprive the victim

[2] The Court’s practice is not to read the full indictment to the jury and not to send the indictment to the jury as part of the Court’s instruction.

[3] Because the Supreme Court and Ninth Circuit have interpreted the similar language of the bank, mail, and wire fraud statutes consistently, this Order relies on precedent analyzing any of the three statutes. *See Carpenter v. United States*, 484 U.S. 19, 25 n.6 (1987); *Neder v. United States*, 527 U.S. 1, 20 (1999); *United States v. Miller*, 953 F.3d 1095, 1102 n.7 (9th Cir. 2020), *cert. denied*, 141 S. Ct. 1085 (2021).

of money or property. *Kelly v. United States*, 140 S. Ct. 1565, 1571 (2020). The specific intent element likewise requires that "defendant must act with the intent not only to make false statements or utilize other forms of deception, but also to deprive a victim of money or property by means of those deceptions." *Miller*, 953 F.3d at 1101. In other words, intent to both "deceive and cheat." *Id.*

With the elements of wire fraud in mind, the Court addresses defendant's arguments that (a) the cryptomining allegations have nothing to do with the data theft allegations, and (b) the cryptomining allegations do not state an offense.

a. Interconnection of Allegations

The defense contends that the cryptomining allegations are irrelevant and immaterial because "the allegation that Ms. Thompson utilized the purported victims' computer systems for the mining of cryptocurrency has no bearing on whether she utilized misconfigurations in the victim's web application firewalls to access stored data without authorization." Dkt. # 124 at 5. This argument is disingenuous.

Count 1 alleges that defendant created proxy scanners that allowed her to identify Amazon Web Services (AWS) servers with misconfigured web application firewalls that permitted outside commands to reach and be executed by the servers. Dkt # 166 at ¶ 12. While concealing her identity utilizing VPNs and TOR,[4] defendant then allegedly sent commands to the misconfigured servers to obtain security credentials for particular accounts and roles belonging to the victims. *Id.* at ¶¶ 11-13, 17-18. Only at this point do the allegations diverge between those related to copying victim data and those related to cryptomining. On the one hand, defendant is alleged to have used these accounts and roles to copy victim data from the servers. *Id.* at ¶¶ 14-16, 19-20. On the other hand, defendant is alleged to have used these accounts and roles to place programs on certain victim servers that allowed her to mine cryptocurrency using "stolen computing power." *Id.* at ¶¶ 21-22.

[4] VPNs (virtual private networks) and TOR (The Onion Router) are both technologies that facilitate online privacy and can be used to conceal a user's identity and/or location.

As alleged, both acts relied on the same technical foundation, and the indictment makes this abundantly clear. Far from being immaterial and irrelevant, the cryptomining allegations independently complete a cohesive theory of the government's wire fraud case.

Defendant's citation to *Yates* and *Kelly* for the premise that loss to the victim "must be an object of [wire] fraud, not a mere implementation cost or incidental byproduct of the scheme," Dkt. # 124 at 5 (quoting *United States v. Yates*, 16 F.4th 256, 264 (9th Cir. 2021)); *see also Kelly*, 140 S. Ct. at 1573-74, is vexing in this context. If a loss is an implementation cost or incidental byproduct, then it stands to reason that the scheme caused the loss. That the Supreme Court has explained that such a loss is insufficient to fulfill the property deprivation requirement of wire fraud does not change this result. Here, defendant asks the Court to conclude that the alleged data theft and cryptojacking are unrelated. A conclusion that the loss caused by one is in fact an implementation cost or incidental byproduct of the other would lead to a result contrary to what defendant seeks. This question, however, is academic in this context. As alleged, the data theft and cryptomining allegations appear to be branches of the same scheme rather than implementation costs or incidental byproducts.

Due to the shared foundation of defendant's alleged data theft and cryptojacking, the argument that the allegations have nothing to do with one another fails.

b. Failure to State an Offense

Defendant also makes a back-door argument that the cryptojacking allegations in Count 1 fail to state an offense. While defendant does not explain the significance of this argument to the surplusage analysis, it appears that this argument goes to the relevance of the cryptojacking allegations. In essence, defendant argues that because the cryptojacking allegations do not independently sustain the charge of wire fraud, they are irrelevant to the charge.

Defendant attacks the cryptojacking theory on the grounds that any computer power or hardware that she is alleged to have consumed by cryptojacking would belong to AWS, as the owner of the servers. AWS is not listed as a victim in the indictment. Defendant argues that this creates a "convergence" problem because the government must allege that she had the requisite intent to "obtain money and property from the one who is deceived," and that it was the enumerated victims, not AWS, who were allegedly deceived. Dkt. # 163 at 5 (citing *United States v. Lew*, 875 F.2d 219, 221 (9th Cir. 1989); *United States v. Ali*, 620 F.3d 1062, 1071 (9th Cir. 2010)).

The Court disagrees that the indictment presents a convergence problem. The Court reads the indictment in its entirety, construes it according to common sense, and interprets it to include facts which are necessarily implied. *United States v. Berger*, 473 F.3d 1080, 1103 (9th Cir. 2007) (quoting *United States v. King*, 200 F.3d 1207, 1217 (9th Cir. 1999)). The indictment alleges that defendant placed cryptojacking programs "on certain victims' servers . . . . Successful mining operations consume large amounts of computing power and hardware." Dkt. # 166 at ¶ 21. Construed according to common sense and interpreted to include facts which are necessarily implied, the indictment alleges that defendant consumed *the victims'* computing power and hardware that they were "renting or contracting" from AWS. *See id.* at ¶¶ 3-10, 21. This is implicit in that the indictment refers to the "victims' servers," not "AWS' servers." *Id.* at ¶ 21. To the extent that defendant argues that she is aware of no evidence that her alleged cryptojacking activities caused any of the enumerated victims any damage such as increased usage invoices, this is a question of fact that can be raised at trial. *See United States v. Kelly*, 874 F.3d 1037, 1046-47 (9th Cir. 2017).[5]

2. Prejudicial or Inflammatory

Because it is dispositive under Rule 7(d) that the cryptomining allegations are material and relevant, the Court need not consider if these allegations are prejudicial or inflammatory. *See Laurienti*, 611 F.3d at 546-47. Nonetheless, the Court also finds that defendant has not shown these allegations are prejudicial or inflammatory. The defense argues that the cryptomining allegations are prejudicial and inflammatory because the government does not

[5] While not dispositive to the question at hand, the Court notes that defendant's claim that she is aware of no evidence that her alleged cryptojacking activities caused damage such as increased usage costs to any of the enumerated victims is contradicted by the evidence that she filed in support of her reply. These emails state that an enumerated victim experienced increased usage costs and explain how the activity that led to the increased bill is consistent with defendant's alleged actions. *See* Dkt. # 164-2 at 1-2. While weighing the evidence must be left to the trier of fact, this is far from "no evidence."

allege that defendant attempted to monetize or profit from the copied data. Therefore, the defense argues, the government's only motivation for including the cryptomining allegations must be to confuse the jury into believing that defendant had intent to deceive and cheat the alleged victims because she had intent to cryptojack.

As the Court discussed in its Order issued February 28, 2022 (Dkt. # 202), it is inconsequential whether defendant attempted to monetize or profit from the data, and intent may be inferred from her alleged pattern of conduct.

First, the law requires that she acted with intent to deprive the victim of "money or property." *Miller*, 953 F.3d at 1101. The data is property, and the law does not ask what she intended to do with it next. *Cf. Carpenter*, 484 U.S. at 26-27.

Second, intent to defraud may be demonstrated through circumstantial evidence. *United States v. Lothian*, 976 F.2d 1257, 1267-68 (9th Cir. 1992) ("It is often difficult to prove fraudulent intent by direct evidence and it must be inferred in such cases from a pattern of conduct or a series of acts, aptly designated as badges of fraud."). The indictment includes numerous allegations of circumstantial evidence of intent.[6] Of these allegations, the majority describe acts common to defendant's alleged data theft and cryptojacking. Defendant's argument that the government is impermissibly leaning on the cryptojacking allegations to prove intent is therefore unpersuasive.

[6] These include: "(1) creating and using scanners that allowed her to identify servers with misconfigured web application firewalls; (2) 'transmitti[ing] commands to the misconfigured servers that obtained the security credentials for particular accounts or roles belonging' to the victims; (3) using the security credentials 'to obtain lists or directories of folders' of data on the victims' cloud storage space; (4) using the stolen credentials 'to copy data, from folders or buckets of data' in the victims' cloud storage space; (5) implicitly representing that the commands she sent to the servers were legitimate and came from a user with permission to send such commands; (6) using VPNs and TOR to conceal her location and identity while taking these actions; and (7) using 'her unauthorized access to certain victim servers—and stolen computing power of those servers—to "mine" cryptocurrency for her own benefit.'" Dkt. # 202 at 10.

Because defendant's argument that the cryptojacking allegations are inflammatory and prejudicial rests on the flawed premise that the government has not otherwise alleged defendant's specific intent, this argument fails.

Defendant has not convinced the Court that Count 1's cryptojacking allegations should be stricken as surplusage under Rule 7(d). Her motion to strike is therefore denied.

B. Count 8

Defendant moves the Court to exercise its discretion pursuant to Federal Rule of Criminal Procedure 14(a) to sever Count 8 of the indictment, or, in the alternative, conduct an evidentiary hearing to determine whether severance is appropriate. Under Rule 14(a), "If the joinder of offenses . . . in an indictment . . . appears to prejudice a defendant . . . the court may order separate trials of counts . . . or provide any other relief that justice requires." Fed. R. Crim. P. 14(a). The Court declines to exercise its discretion to sever Count 8 or order an evidentiary hearing, as defendant has not shown such relief is warranted.

Count 8 alleges that defendant violated the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030. In particular, Count 8 alleges that defendant knowingly caused the transmission of a program, code, and commands designed to perform cryptomining and to delete the code, logs, and other records of the cryptomining and, as a result of such conduct, intentionally caused damage without authorization to protected computers in violation of 18 U.S.C. § 1030(a)(5)(A). Dkt. # 166 at ¶ 31.

Defendant contends that Count 8 should be severed because the government improperly uses it as a stalking horse for intent. Defendant presents four supporting arguments, which the Court considers in turn: (1) Count 8 is insufficiently detailed compared to the other Counts, (2) there is no evidence to support Count 8, (3) Count 8 is dissimilar to the other Counts, and (4) Count 8 does not state an offense.

1. Detail of Allegations

Defendant argues that Count 8 should be severed as prejudicial because it improperly serves as a malicious intent "catch-all" given that it is less detailed than the Counts 2 through 7, 9, and 10. This argument lacks merit.

First, defendant does not explain how less detail equates to serving as a stalking horse for intent. Second, even assuming that it does, Count 8 is no less detailed than these other Counts. Count 8 identifies two particular victims: Victim 7 and Victim 8. That it also refers to "other victims" is not a condemning lack of information. Dkt. # 166 at ¶ 31. It gives the dates of the alleged scheme: "on or before March 10, 2019, and continuing until on or after August 5, 2019." *Id.* That the scheme may have been ongoing over an extended period of time does not somehow negate the dates. Defendant's assertion that the other Counts allege "the exact type of data stolen" is puzzling because Counts 2-7 merely allege that defendant obtained "information from a protected computer" belonging to the enumerated victims.[7] *Id.* at ¶¶ 25, 27, 29, 33, 35. In contrast, Count 8 explains that the program, code, and commands that defendant allegedly transmitted to the computers was designed to perform cryptomining and then delete the code, logs, and other records of the cryptocurrency mining. *Id.* at ¶ 31. This is more, not less, detail of how defendant is alleged to have interacted with the protected computers than is given in the other CFAA Counts. Finally, defendant does not explain why the indictment should include the "amounts of cryptocurrency mined." Dkt. # 124 at 7. This argument therefore fails.

2. Evidence

Defendant argues in her reply that Count 8 should be severed as prejudicial because "[t]he evidence against Ms. Thompson under Count 8 is non-existent even though the 'government [claims it] has provided full discovery.'" Dkt. # 163 at 7 (quoting Dkt. # 131 at 3). Requests to sever under Rule 14(a) are not constrained to the four corners of the indictment. *See United States v. Jawara*, 474 F.3d 565, 573-74 (9th Cir. 2007). Nonetheless, this argument fails.

First, the defense again fails to explain *why* a lack of evidence means the charge is prejudicial. If the government's plot is supposedly to use Count 8 to make defendant appear malicious and thus confuse the jury into cumulating the evidence of intent between the wire

[7] Count 2 also alleges that defendant obtained "information contained in a financial record of a financial institution." Dkt. # 166 at ¶ 25. Counts 9 and 10 are not CFAA Counts and do not directly allege that defendant stole data. *Id.* at ¶¶ 33, 35.

fraud and CFAA charges, *see* Dkt. # 163 at 7 (citing *United States v. Johnson*, 820 F.2d 1065, 1070 (9th Cir. 1987) (stating severance is necessary where "jury may cumulate the evidence of the various crimes charged and find guilt when, if considered separately, it would not so find")), this would be a poor plot without any supporting evidence. Second, the government has provided evidence. *See* Dkts. # 175 at 2, # 176. The weighing of this evidence is best left to the jury.

3. Similarity to Other Counts

Defendant argues that Count 8 should be severed because the indictment does not suggest that the charges of cryptomining, on the one hand, and unauthorized access and theft of stored data, on the other, "either depended upon or necessarily led to the commission of the other," or were of "similar character." Dkt. # 124 at 8 (quoting *Jawara*, 474 F.3d at 574, 578). While defendant cites only the Court's discretion under Rule 14(a) to sever Count 8, this argument invokes the propriety of the joinder under Rule 8(a).[8] Nonetheless, even if the Court construes this as a request pursuant to Rule 8(a), this argument fails.

Under Rule 8(a), joinder of offenses in the indictment against a single defendant is proper if the offenses charged are (1) "of the same or similar character," (2) "based on the same act or transaction," or (3) "connected with or constitut[ing] parts of a common scheme or plan." *Jawara*, 474 F.3d at 572 (quoting Fed. R. Crim. P. 8(a)). The validity of the joinder under Rule 8(a) is determined solely by the allegations in the indictment. *Id.* (quoting *United States v. Terry*, 911 F.2d 272, 276 (9th Cir. 1990)).

Here, the joinder of Count 8 satisfies Rule 8(a) because the offenses as alleged in the indictment constitute parts of a common scheme or plan. "[C]ourts generally permit joinder under this test where the counts 'grow out of related transactions.'" *Id.* at 574 (quoting *United*

[8] In support of this argument, defendant cites to portions of *Jawara* analyzing Rule 8(a) and quotes language echoing its mandate. *Compare* Fed. R. Crim. P. 8(a) ("The indictment . . . may charge a defendant in separate counts with 2 or more offenses if the offenses charged . . . are of the same or similar character, or are based on the same act or transaction, or are connected with or constitute parts of a common scheme or plan.") *with* Fed. R. Crim. P. 14(a) ("If the joinder of offenses . . . in an indictment . . . appears to prejudice a defendant . . . the court may order separate trials of counts . . .").

States v. Randazzo, 80 F.3d 623, 627 (1st Cir. 1996)). "When the joined counts are logically related, and there is a large area of overlapping proof, joinder is appropriate." *Id.* (quoting *United States v. Anderson*, 642 F.2d 281, 284 (9th Cir. 1981)). As explained in Section II.A.1.a. above, the cryptojacking and data theft allegations are closely intertwined because they rely on the same underlying course of action and technical underpinnings. This analysis remains true in relation to the CFAA, access device fraud, and aggravated identity theft Counts, which reallege and incorporate all allegations set forth in Count 1. *See* Dkt. # 166 at ¶¶ 24, 26, 28, 30, 32, 34. The Counts are related as they share initial steps and will undoubtedly require overlapping proof.[9] Joinder is therefore appropriate. Because only one of Rule 8(a)'s three conditions must be satisfied for joinder to be appropriate, *see Jawara*, 474 F.3d at 572, the Court need not consider whether the offenses are also of the same or similar character or based on the same act or transaction. This argument therefore fails.

4. Statement of an Offense

Defendant again makes a back-door argument that Count 8 does not state an offense. Defendant argues that Count 8 does not allege a CFAA violation because it does not allege that defendant accessed a computer without authorization. Therefore, the argument goes, its presence in the indictment must be solely to suggest a potential motive for the other CFAA Counts. This argument is without merit. The other CFAA Counts allege that that defendant violated 18 U.S.C. § 1030(a)*(2)(C)*, which requires that defendant "intentionally *accesse[d] a computer without authorization* or exceed[ed] authorized access." 18 U.S.C. § 1030(a)(2)(C) (emphasis added); *see* Dkt. # 166 at ¶¶ 25 (Count 2), 27 (Counts 3-5), 29 (Counts 6-7). In contrast, Count 8 alleges that defendant violated 18 U.S.C. § 1030(a)*(5)(A)*, which requires that defendant "knowingly cause[d] the transmission of a program, information, code, or command, and as a result of such conduct, *intentionally cause[d] damage without authorization*, to a

[9] For example, while the Court conducts this Rule 8(a) analysis based solely on the indictment, the government contends that defendant's social media, text, and chat communications discussing her alleged cryptojacking activities are important evidence to show that she is the person who accessed AWS's servers for the purposes of the data theft allegations. Dkt. # 138 at 13.

protected computer." 18 U.S.C. § 1030(a)(5)(A) (emphasis added); *see* Dkt. # 166 at ¶ 31 (Count 8). There is no sinister motive to be read into the fact that separate charges require proof of different elements.

Defendant's citation to *Van Buren* for the proposition that "[t]he only intent relevant under the CFAA is the intent in accessing the computer system, not the actions that occur after such access occurs," Dkt. # 163 at 6 (citing *Van Buren v. United States*, 141 S. Ct. 1648, 1652 (2021)), is equally misplaced. *Van Buren* analyzes 18 U.S.C. § 1030(a)*(2)*. *Van Buren*, 141 S. Ct. at 1652. As discussed in the immediately preceding paragraph, this is not the subsection of the CFAA under which Count 8 is charged, and the applicable subsection has a different intent requirement: "intentionally caus[ing] damage without authorization." 18 U.S.C. § 1030(a)(5)(A). This argument therefore fails.

As all of defendant's arguments requesting the Court to sever Count 8 fail, defendant's motion to sever is denied. Because an evidentiary hearing would not alter this result, defendant's request for an evidentiary hearing is denied.

III. Conclusion

For all of the foregoing reasons, IT IS HEREBY ORDERED that:

1. Defendant's Motion to Strike the Crypto Mining Allegations of Count One and to Sever Count Eight of the Indictment (Dkt. # 124) is DENIED.
2. The government's Motion to File a Brief in Excess of Twelve Pages (Dkt. # 136) is GRANTED.
3. Defendant's Motion to File Overlength Reply Re Defense Motion to Strike Count 1 and Sever Count 8 (Dkt. # 161) is GRANTED.
4. Defendant's Motion to Seal Exhibits to Defendant's Reply to Government's Response to Motion to Strike Count 1 and Sever Count 8 (Dkt. # 162) is GRANTED.
5. The government's Motion to Seal Exhibit A to Supplemental Filing Relating to Defendant's Motion to Strike Cryptojacking Allegations and to Sever Count 8 (Dkt. # 174) is GRANTED.

6. Defendant’s Motion to Strike Government’s Surreply (Dkt. # 184) is GRANTED IN PART. Paragraph 2 of the government’s surreply (Dkt. # 175) is stricken.

DATED this 21st day of March, 2022.

Robert S. Lasnik
United States District Judge